REPLACEMENT DRAWINGS

Please replace all of the original 22 sheets with eight Replacement Sheets submitted herewith as follows:

sheet 1 – canceled
sheet 2 – canceled
sheet 3 – canceled
sheet 4 – canceled
sheet 5 – canceled
sheet 6 – canceled
sheet 7 – canceled
sheet 8 – canceled
sheet 9 – canceled
sheet 10 – canceled
sheet 11 – canceled
sheet 12 (Figs. 13, 13a) – renumbered as Replacement Sheet 6 (Figs. 6, 6a)
sheet 13 (Fig. 14) – canceled
sheet 14 (Fig. 15) – canceled
sheet 15 (Figs. 16, 16a) – renumbered as Replacement Sheet 7 (Figs. 7, 7a)
sheet 16 (Fig. 17) – canceled
sheet 17 (Fig. 18) – renumbered as Replacement Sheet 8 (Fig. 8)
sheet 18 (Fig. 19) – renumbered as Replacement Sheet 1 (Fig. 1)
sheet 19 (Fig. 20) – renumbered as Replacement Sheet 2 (Fig. 2)
sheet 20 (Fig. 21) – renumbered as Replacement Sheet 3 (Fig. 3)
sheet 21 (Fig. 22) – renumbered as Replacement Sheet 4 (Fig. 4)
sheet 22 (Fig. 23) – renumbered as Replacement Sheet 5 (Fig. 5)

In Fig. 3, ~~telephone system~~ is changed to other network.
In Fig. 6, 6a, error ~~126~~ deleted, ~~53~~ to 104, ~~from disk 43~~, ~~game~~ to chip, ~~50~~ to 86.
In Fig. 7, 7a, ~~132~~ to 96, ~~A from disk~~, ~~Enhancement~~ to Download.
In Fig. 8, ~~132~~ to 96.

REMARKS and ARGUMENTS

This is a Response to the non-final Office Action mailed February 9, 2007.

Claims 90–108 are pending

Substitute Specification and Replacement Drawings

Applicant has canceled 14 drawings and deleted corresponding paragraphs in the original Specification and herewith submits a Substitute Specification and full set of eight replacement drawings that that show and describe the claimed invention. Original paragraph numbers have been retained wherever possible, as summarized on page 5 of this Response. The eight replacement drawings are identical to eight original drawings except for renumbered Figure numbers, sheet numbers, and 4 minor amendments, as detailed on page 4 of this Response. No new matter has been introduced by these amendments.

Claim Objections

In the Office Action mailed February 9, 2007, claims 11 and 12 were rejected for lack of antecedent basis. Claims 11 and 12 have been canceled and therefore the issue is moot.

Claim Rejections – 35 USC § 112

In the Office Action mailed February 9, 2007, claims 1, 11, and 21 were rejected for failing to distinctly claim the invention. Claims 1, 11, and 21 have been canceled and therefore the issue is moot.

Claim Rejections – 35 U.S.C. § 103

In the Office Action mailed February 9, 2007, independent claims 1, 21, 27, 33, 35, 59, 65, 70 and 85, and some claims dependent thereon, were rejected under 35 USC § 103(a) as being unpatentable over Eliott (US 6,712,704) hereinafter "Eliott", in view of Ishibashi et al. (US 6,728,379) hereinafter "Ishibashi".

Applicant has canceled all prior claims 1–89 and herewith submits new claims 90–108 that are limited to decryption and execution of downloaded encrypted program instructions in a "secure cryptoprocessor" that prevents physical and electronic access to the decrypted instructions and other secret data from outside of the secure cryptoprocessor. Claims dependent on the canceled examined claims are canceled and therefore the obviousness issues thereon are moot. Neither Eliott nor Ishibashi show, describe, or remotely suggest use of a secure cryptoprocessor as defined in applicant's new claims 90, 100, and 104.

Prior-art secure cryptoprocessors are described in Best (US patent 4,278,837) and are manufactured by Dallas Semiconductor Corporation, a subsidiary of Maxim Integrated Products. Wherever "cryptoprocessor" appears in the present claims, "secure cryptoprocessor" is implied.

Subject to said secure cryptoprocessor limitation, applicant retains the full scope of equivalents as indicated in paragraph [0110] of the Substitute Specification.

As noted by the Examiner, Eliott discloses a method of securely distributing programs from a server for execution in an electronic game system and comprises the steps of storing the program in a server, encrypting the program in a server processor under control of an encryption key, transferring the encrypted program from the server to a second processor chip, decrypting a session key in the second processor chip, decrypting the encrypted game program under control of the decrypting key to produce executable digital instructions stored in the second processor chip, and executing the decrypted instructions in the second processor chip to produce game data.

Also as noted by the Examiner, Eliott does not disclose storing a decryption key corresponding to the encryption key, encrypting the decryption key in the first processor in the server to produce an encrypted decryption key, transferring the encrypted decryption key, or decrypting the encrypted decryption key to reproduce the decryption.

As further noted by the Examiner, Ishibashi discloses storing a decrypting key corresponding to the encrypting key, encrypting the decrypting key in the first processor to produce an encrypted decryption key, transferring the encrypted decrypyion key, and decrypting the encrypted decryption key to reproduce the decryption key.

Although applicant's original specification clearly specified the elements of a secure cryptoprocessor in paragraphs [0005], [0093], and [0098], this limitation was not clearly expressed in applicant's examined claims (now canceled). Applicant's pending claims include the structure of a secure cryptoprocessor in each independent claim 90, 100, and 104. Wherever the word "cryptoprocessor" appears in applicant's claims, a secure cryptoprocessor is implied. The cryptography processor 130 in Ishibashi and security processor 180 in Eliott are not secure cryptoprocessors, as this term is defined in applicant's claims.

In the preamble of applicant's claim 90, the clause "which are inaccessible from said secure cryptoprocessor chip" means that the decrypted program instructions are not accessible from the secure cryptoprocessor chip, except during fabrication and testing by the chip manufacturer or its agent. This limitation is not shown, described, or suggested in Eliott or Ishibashi.

Eliott discloses a server 101 that encrypts a program as a function of a unique ID (Fig. 11, column 26, lines 28–31), transfers the encrypted program to game device 95 where the encrypted program is stored on hard drive 206 (col 26, lines 34–35), decrypts the encrypted program in a second game system 50 (col 26, lines 33–35) to produce executable program instructions, and then reveals these decrypted instructions in the "CLEAR" (Fig. 11) for execution in the second game system 50 in CPU 100 and GPU 200 (Fig. 2). By specifying that the decrypted instructions are in the "CLEAR" in system 50, Eliott teaches away from secure cryptoprocessors.

In secure cryptoprocessors, the decrypted instructions are executed in the same secure cryptoprocessor that decrypts them. The decrypted instructions are not accessible from the cryptoprocessor chip. This is an expressed limitation in applicant's claims that is not shown, described, or remotely suggested in Eliott.

Moreover, Eliott specifies storing the "unique ID" in disk drive 206 (Fig. 11) which would make the unique ID ("which can't be read by a user" col 26, line 24–26) accessible to software pirates who open the disk drive. There is no suggestion in Eliott that this problem may be solved by storing the unique ID in the same processor that decrypts and executes the downloaded instructions.

Applicant's claims further specify encrypting the decryption key (not the program) as a function of the unique ID, in contrast to the teachings of Eliott in which "the server uses the unique ID as a key to encrypt the game" program (col 26, lines 28–31).

In summary, Eliott lacks:

1) a secure cryptoprocessor (as defined in applicant's claims 90, 100, and 104),
2) executing decrypted instructions in the same processor that decrypts them,
3) physical and electronic inaccessibility of the decrypted instructions,
4) storing a unique ID in a secure cryptoprocessor,
5) a program decryption key that is different than the unique ID, and
6) downloading an encrypted decryption key separately from the encrypted program.

As noted by the Examiner, Ishibashi (US 6,728,379) discloses: decrypting an encrypted decryption key (col 2, lines 17–18) to produce the program decryption key; to store the program decryption key (col 2, lines 15–16); encrypting the program decryption key (col 7, lines 43–46) under control of another key (col 7, lines 59–61); and transferring the encrypted decryption key (col. 2, lines 23–25).

Ishibashi discloses a cryptography processor, but does not show, describe, or remotely suggest a secure cryptoprocessor having the structure defined in applicant's claims. Ishibashi does not mention "execute" or "execution" or "instruction"(s) or "unique" or "ID" or "ident" or "access", and therefore lacks several of the features also lacking in Eliott:

1) a secure cryptoprocessor,
2) executing decrypted instructions in the same processor that decrypts them,
3) physical and electronic inaccessibility of the decrypted instructions,
4) storing a unique ID in a secure cryptoprocessor, and
5) a program decryption key that is different than the unique ID.

Moreover, Ishibashi teaches away from secure cryptoprocessors by referring to "program" as mere content such as "music, image, program, text, etc." (col 1, lines 19–21). Secure cryptoprocessrs are based on the fact that unlike music, images, video, and text, computer program instructions in decrypted form need not be revealed to end users and therefore can be made inaccessible. There is no suggestion in Ishibashi that decrypted program instructions should be inaccessible outside of cryptographic processor 130.

It is not clear in Ishibashi whether "program" means a television show or computer program. Because Fig. 8 in Ishibashi shows decrypted "content" i.e. programs, being output to video recorder 270 and the words "execute" or "execution" or "instruction"(s) that would suggest a computer program do not appear in Ishibashi, the teachings of Ishibashi do not rise to the "objective teaching" required in Ex parte Levengood, 28 U.S.P.Q. 2d 1300 (P.T.O.B.A.&I. 1993) which states that the Patent and Trademark Office "can satisfy the burden of establishing a *prima facie* case of obviousness only by showing some objective teaching in either the prior art, or knowledge generally available to one of ordinary skill in the art, that would lead that individual to combine the relevant teachings of the references."

Ishibashi fails to teach all of the above described features and limitations in applicant's claims that are also lacking in Elliott. Therefore, applicant submits that it would not have been obvious to one of ordinary skill in the art at the time of applicant's priority date to design applicant's invention by combining the teachings of Eliott and Ishibashi.

Best (US patent 4,278,837) discloses a secure cryptoprocessor, execution of decrypted program instructions in the same secure cryptoprocessor that decrypts them, writeable memory for storing decrypted instructions, and block encryption/ decryption under control of digital keys to produce decrypted instructions that are inaccessible outside of the chip. Best lacks a unique chip id, network server, and network transmission.

If the teachings of Eliott, Ishibashi, and Best were combined, the combination would not show, describe, or suggest the following limitations in applicant's claims 90, 100, and 104:

1) storing a unique ID in a secure cryptoprocessor, as the word cryptoprocessor is defined in applicant's claims,

2) a program decryption key that is different than the unique ID,

3) encrypting a unique ID together with a decryption key,

4) decryption in a secure cryptoprocessor of executable program instructions that are transmitted from a network server in encrypted form.

5) decryption in a secure cryptoprocessor of executable program instructions under control of a decryption key that is transmitted from a network server in encrypted form.

6) decryption in a secure cryptoprocessor of an encrypted decryption key that is transmitted from a network server in encrypted form,

7) execution in a secure cryptoprocessor of program instructions that are transmitted from a network server to the secure cryptoprocessor in encrypted form.

In order to establish a *prima facie* case of obviousness, all of the claim limitations must be taught or suggested by the prior art references when combined (MPEP 706.02(j)). Even if the teachings of Best were combined with the teachings of Eliott and Ishibashi, the combination would not teach or suggest all of the claim limitations.

In view of the above, each of the presently pending claims in this application is believed to be in condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue.

Respectfully submitted,

GRAYBEAL JACKSON HALEY LLP

Jeffrey T. Haley
Registration No. 34,834
155 - 108th Avenue N.E., Suite 350
Bellevue, WA 98004-5901

(425) 455-5575.